Please find below and/or attached an Office communication concerning this application or proceeding.

	Office Action Summary	Application No.	Applicant(s)
		09/931,550	GOODMAN ET AL.
		Examiner	Art Unit
		Andrew L Nalven	2134

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _16 August 2001_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-19_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) _19_ is/are allowed.

6)☒ Claim(s) _1-18_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _16 August 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _8/16/01_.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

1.   Claims 1-19 are pending.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2.   Claims 10-17 are rejected under 35 U.S.C. 101 because the cited claims are directed to a computer program product that is adapted for storage on a computer readable medium. Examiner notes that claim language such as "adaptable" merely suggests limitations or makes limitations optional. In using claim language such as "adaptable" applicant has not required steps to be performed or limited an apparatus to a particular structure (see MPEP 2106). Thus, the cited claims fail to provide an invention with a useful, concrete, and tangible result.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section

351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4.   Claims 1-3, 7-12, 16-17 are rejected under 35 U.S.C. 102(e) as being anticipated

by Alexander et al US Patent No. 6,188,602. Alexander teaches a mechanism to

commit data to a memory device with read-only access.

5.   With regards to claims 1 and 10, Alexander teaches the receiving of a request to

unlock the utility (Alexander, column 5 lines 46-52, operating system requests access to

flash), verifying an update to the utility (Alexander, column 5 lines 58-61, verify the

data), and using a system management interrupt handler to query a status of the

verifying step (Alexander, column 5 lines 58-61, smi access state verifies data).

6.   With regards to claims 2 and 11, Alexander teaches that the step of unlocking the

utility and updating the utility if verifying step successfully verifies the update of the utility

(Alexander, column 5 lines 41-45, if valid RBU image exists allow loading).

7.   With regards to claims 3 and 12, Alexander teaches the step of not unlocking the

utility if the verifying step fails to verify the update to the utility (Alexander, column 5

lines 34-42).

8.   With regards to claims 7 and 16, Alexander teaches the locking of the utility with

the SMI handler after the utility has been updated (Alexander, column 5 lines 62-64).

9.   With regards to claim 8, Alexander teaches the utility being a flash utility

(Alexander, column 5 line 61, flash memory).

10.   With regards to claims 9 and 17, Alexander teaches the requesting step being

performed by an SMI handler (Alexander, column 5 lines 58-62, receiving a request).

Claim Rejections - 35 USC § 103

11.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

12.   Claims 4-6, 13-15, and 18 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Alexander et al US Patent No. 6,188,602 in view of Grawrock US

Patent No. 6,678,833. Grawrock discloses a system for the protection of boot block

data.

13.   With regards to claims 4 and 13, Alexander fails to teach the verifying being

performed by a trusted platform module (TPM) in accordance with the Trusted

Computing Alliance Specifications. Grawrock teaches verifying being performed by a

trusted platform module (TPM) in accordance with the Trusted Computing Alliance

Specifications (Grawrock, column 4 lines 1-9, verification by a challenger). At the time

the invention was made, it would have been obvious to a person of ordinary skill in the

art to utilize Grawrock's method of using a trusted platform module because it offers the

advantage of allowing the TPM to accurately report the identity of the boot block or

utility without reliance on any intervening devices (Grawrock, column 2 lines 1-6).

14.   With regards to claims 5 and 14, Alexander as modified teaches the SMI handler

used to query the status of the verifying step queries the TPM for status (Alexander,

column 5 lines 58-61, Grawrock, column 4 lines 1-9).

15.   With regards to claims 6 and 15, Alexander as modified teaches the SMI handler

being issued by the TPM (Alexander, column 5 lines 58-61, Grawrock, column 4 lines 1-

9).

16.   With regards to claim 18, Alexander teaches a processor (Alexander, column 2

lines 56-57), a BIOS utility stored in flash memory coupled to the processor (Alexander,

column 3 lines 45-46), input circuit for receiving an update to the BIOS utility

(Alexander, column 5 lines 11-13), a bus system for coupling the input circuit to the

processor (Alexander, column 3 lines 6-24), a BIOS update application requesting an

unlock of the flash memory from a system management interrupt (SMI) handler

(Alexander, column 5 lines 58-61), the SMI handler unlocking the flash memory if the

SMI handler sets the status as successful (Alexander, column 5 lines 58-61 and 42-46),

the BIOS update application updating the BIOS utility with the update (Alexander,

column 5 lines 42-46), and the SMI handler locking the flash memory after the update of

the BIOS utility has completed (Alexander, column 5 lines 62-64). Alexander fails to

teach the use of a trusted platform module (TPM) and the requesting of cryptographic

verification of the BIOS. Grawrock teaches a trusted platform module coupled to the

processor and operating under the Trusted Computing Platform Alliance Specifications

(Grawrock, column 3 lines 50-57, column 1 lines 24-36), the requesting of cryptographic

verification of the BIOS utility update from the TPM (Grawrock, column 3 lines 1-18,

hash operation, boot block identifier), the TMP including programming for issuing an

SMI to query the TPM for a status on the verifying of the authenticity of the BIOS utility

update (Alexander, column 5 lines 58-61, Grawrock, column 4 lines 1-9). At the time

the invention was made, it would have been obvious to a person of ordinary skill in the

art to utilize Grawrock's TPM with Alexander's memory device because it offers the

advantage of allowing the TPM to accurately report the identity of the boot block or

utility without reliance on any intervening devices (Grawrock, column 2 lines 1-6).

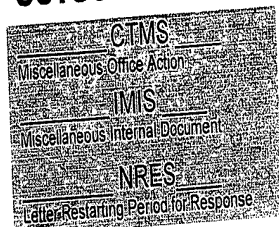## Allowable Subject Matter

17.   Claim 19 is allowed.

18.   The following is a statement of reasons for the indication of allowable subject

matter: The cited prior art, Alexander and Grawrock, fail to teach or suggest the distinct

feature of setting a status flag to pending if a verification of the update to the flash utility

has not completed where the verification is requested by a Trusted Platform Module by

way of a system management interrupt. Thus, the cited prior art fails to anticipate or

render obvious the above-cited claim.

Conclusion

19.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Andrew L Nalven whose telephone number is 571 272

3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate

Fridays.

OUTGOING DOCUMENT INDEX SHEET

A DOCPHOENIX

OUTGOING

_____ CTMS _____
Miscellaneous Office Action

_____ IMIS _____
Miscellaneous Internal Document

_____ NRES _____
Letter Restarting Period for Response

_____ 1449 _____
Signed 1449

_____ 892 _____
892

_____ ABN _____
Abandonment

_____ APDEC _____
Board of Appeals Decision

_____ APEA _____
Examiner Answer to Appeal Brief

_____ CRFR _____
Letter Requiring CRF

_____ CTAV _____
Count Advisory Action

_____ CTEQ _____
Count Ex parte Quayle

_____ CTFR _____
Count Final Rejection

_____ CTNF _____
Count Non-Final

_____ CTRS _____
Count Restriction

_____ EXIN _____
Examiner Interview

_____ FOR _____
Foreign Reference

_____ M903 _____
DO/EO Acceptance

_____ M905 _____
DO/EO Missing Requirement

OUTGOING

_____ NFDR _____
Formal Drawing Required

_____ NOA _____
Notice of Allowance

_____ NPL _____
Non-Patent Literature

_____ PEFN _____
Pre-Exam Formalities Notice

_____ PETDEC _____
Petition Decision

_____ ANE.I _____
After Final or 312 Amendment

_____ PGEA.G _____
Petition Decision Express ABN

_____ XRUSH _____
TC Resp. to Printer Query

PTO INTERNAL

_____ CLMPTO _____
PTO Prepared Complete Claim Set

_____ IIFW _____
File Wrapper Issue Information

_____ SRNT _____
Examiner Search Notes

_____ SRFW _____
File Wrapper Search Info

_____ SEQREQ _____
Sequence Problem Att. from Examiner

_____ CDCHECK _____
Compact Disk Review Checklist

---

y telephone are unsuccessful, the examiner's

d on 571 272 3838. The fax phone number

or proceeding is assigned is 703-872-9306.

application may be obtained from the

IR) system. Status information for

either Private PAIR or Public PAIR.

is is available through Private PAIR only.

see http://pair-direct.uspto.gov. Should

AIR system, contact the Electronic

ee).

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100